UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,428	10/21/2003	Gerard Anthony Brady	026970-003310US	9179

20350 7590 03/17/2008

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
03/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,428	BRADY ET AL.	
	Examiner	Art Unit	
	SHANTO M Z ABEDIN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 34-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 34-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication filed on 12/05/2007.

2. Claims 1- 15 and 34-51 are pending in the application.

3. Claims 1- 15 and 34-51 have been rejected.

Response to Arguments

4. Regarding 35 USC 102 (e) type rejections under Graham et al (US 7237264 B1) , the applicant primarily argues that reference Graham et al fails to disclose detecting an occurrence of a security event within a customer network, wherein detecting includes ascertaining at least one parameter associated with the security event and determining an importance of the security event based on the parameter; and querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step; and analyzing the security event using at least one of the first data and the additional data.

In response to the applicant's above arguments, the examiner respectfully disagrees with the applicant since upon further examination, reference Graham et al was found to teach the above limitations (please see below for detail explanation). Furthermore, upon further examination and search new grounds of rejection are found, and the applicant's above arguments are further moot in view of new grounds of rejection presented in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the

subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1- 15 and 34-51 are rejected under 35 USC 103 (a) as being unpatentable over Graham et al (US 7237264 B1) in view of Porras et al (US 6704874 B1)

Regarding claims 1 and 15, Graham et al discloses a method for analyzing a security event in a distributed fashion, comprising:

(a) detecting an occurrence of a security event within a customer network, wherein detecting includes ascertaining at least one parameter associated with the security event and determining an importance of the security event based on the parameter (Col 4,line 29).

[Graham et al teaches (see Col 4, lines 30-58) at least one factor, or variable, or event/ incident type associated with various network events; Graham further discloses each of these variables/ factors, alone or in combination determines whether an alert condition exists, or what should be the extent of a response to a particular event type ; Therefore, Graham et al's teachings of factors or variables or types associated with the extent of alert condition/ suspiciousness of network events can be interpreted as parameters associated with the security event to determine importance of the security event]

(b) querying a first component of the customer network for data in response to the detected occurrence of the security event (Col 8, starts at line 5; Col 13, starts at line 6; Claim 1; request/ response from target, or acquiring aggregation level or ranked value);

(c) receiving, by a data monitor located within the customer network, first data from the component in response to the query (Col 4, starts at line 50; Col 13, starts at line 6);

(d) determining, based on the received first data, whether to query for additional data (Col 4, starts at line 50; each of these variables alone or in combination, may dictate the type and extent of a response; Col 13, starts at line 6; analysis);

(e) querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step (Col 4, starts at line 30; Col 12, starts at line 50; Claim 1, 9);

[Graham et al discloses querying, and acquiring one or more, or variety of variables or factors associated with the network event from at least one of the network node and another network node or gateway; Graham et al further discloses combining various alerts (types), and determining level or extent or alert of the event based on variety of factors/ variables (see Col 4, starts at line 30; Claim 9) ; Graham et al further discloses acquiring additional data for authentication to determine the event's suspicion level (see Col 13, starts at line 35). Therefore, Graham et al teaches querying, and gathering additional authentication data, or varieties of alerts or factors or variables to determine the security risk level of the network incident]

(f) analyzing the security event using at least one of the first data and the additional data (Col 4, starts at line 50; Col 12, starts at line 50; Claim 1-12; analyzing and assigning alerts/ condition based on varieties of factors/ variables related to the event; Graham et al further discloses acquiring additional data for authentication to determine the event's suspicion level).

In the case, position of the inherency regarding "wherein detecting includes ascertaining at least one parameter associated with the security event and determining an importance of the security event based on the parameter" and "querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step"

are not found supportable, the examiner notes, newly found reference Porras et al teaches wherein detecting includes ascertaining at least one parameter associated with the security event and determining an importance of the security event based on the parameter (Col 2, line 38 to Col 6, line 58; Claims 23-25; plurality of parameters or criteria associated with/ used to determine severity of an attack); and querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step (Col 2, line 38 to Col 6, line 58; Claims 23-25; aggregating alert parameters, or additional records to determine or generate alert/ incident reports regarding the severity of the attack)

Porras et al and Graham et al are analogous art because they are from the same field of endeavor of preventing network intrusions/ attacks. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teachings of Porras et al with Graham et al to design a method w wherein detecting includes ascertaining at least one parameter associated with the security event and determining an importance of the security event based on the parameter, and to obtain the additional data in response to the determining step in order to generate a more accurate attack level and prevention mechanism.

Regarding claim 2, Graham et al discloses the method of claim 1 wherein step (a) further comprises determining at least one of intrusion of the customer network, a port scan, service probes, a signature from an attack, a buffer overflow attempt, a format string attack, a denial of service attempt, a web-based attack, and an attempted rights escalation (Col 6, starts at line 55; Col 9, starts at line 50; port scan; buffer overflow; signature attack etc).

Regarding claim 3, Graham et al discloses the method of claim 1 wherein step (a) further comprises monitoring the customer network for the security event (Col 4, starts at line 40; Col 13, starts at line 6; claims 19,28,31; monitoring).

Regarding claim 4, Graham et al discloses the method of claim 1 wherein step (a) further comprises determining at least one of nature of the security event, likelihood that the security event is harmful, and impact of the security event (Col 6, starts at line 55; Col 9, starts at line 50; claims 19, 28, 31; monitoring/ determining attacks/ alerts).

Regarding claim 5, Graham et al discloses the method of claim 1 wherein step (a) further comprises detecting, by the data monitor, the occurrence of the security event. (Col 9, starts at line 50; claims 19, 28; monitoring/ determining attacks/ alerts).

Regarding claim 6, Graham et al discloses the method of claim 1 wherein the security event further comprises a potential security event (Col 6, starts at line 55; Col 9, starts at line 50; claims 19, 28, 31).

Regarding claim 7, Graham et al discloses the method of claim 1 wherein at least one of the first component and the another component of the customer network further comprises at least one of the data monitor and a client computer (Col 4, starts at line 30; Col 12, starts at line 50; client node; monitoring device/ gateways/ server).

Regarding claim 11, Graham et al discloses the method of claim 1 wherein step (d) further comprises determining, by the data monitor, whether to query for additional data (Col 4, starts at line

30; Col 12, starts at line 50; Claim 1, 9; Graham et al teaches querying, and gathering additional authentication data, or varieties of alerts or factors or variables to determine the security risk level of the network incident)

Regarding claim 12, Graham et al discloses the method of claim 1 wherein step (f) further comprises populating a trouble ticket during the analysis (Col 12, starts at line 50; Claim 1; assigning alert conditions and rank value; the examiner interprets Graham et al 's teachings of assigning alert conditions and rank value as assigning trouble ticket based on the analysis).

Regarding claims 8-10 and 13-14, they recite the limitations of claims 1-7, therefore, they are rejected applying as same as applied rejecting claims 1-7.

Regarding claim 34, Graham et al discloses wherein analyzing the security event is performed by a security analysis module that is not part of the customer network (Col 4, starts at line 30; Col 12, line 15 to Col 13, line 67; firewall/ gateways to monitor client/ target).

Regarding claim 35, Graham et al discloses wherein the parameter conveys what type of security event is detected (Col 4, starts at line 30; factors including type of event). Furthermore, Porras et al teaches wherein the parameter conveys what type of security event is detected (Col 2, line 38 to Col 6, line 58; Claims 23-25; parameters)

Regarding claim 36, Porras et al teaches wherein the parameter includes an amount of time elapsed since an occurrence of a previous security event (Col 2, line 38 to Col 6, line 58; Claims 23-25; parameter including timestamp).

Regarding claim 37, Porras et al discloses wherein the parameter includes a communication protocol associated with the security event (Col 5, starts at line 12)

Regarding claim 38, Porras et al discloses wherein the parameter includes a duration of time of the security event (Claims 23-25; timestamp).

Regarding claim 39, Graham et al discloses wherein the parameter includes a number of previous occurrences of the security event (Col 13, line 50 to Col 14, line 25; determining risk level based on additional information regarding failed/ incorrect login).

Regarding claims 40-51, they recite the limitations of claims 1-7, 15 and 34-39, therefore, they are rejected applying as same as applied rejecting claims 1-7, 15 and 34-39.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136